1

5

7

8

9

10

11

12

13

1415

16

17

18 19

20

21

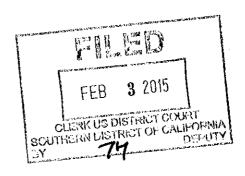
2223

24

25

2627

28



UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

VS.

ROBERTO SOTELO (5),

Defendant.

CASE NO. 13cr4514-BEN

ORDER DENYING MOTION TO SUPPRESS [Dkt. No. 181]

Now before the Court is Defendant's motion to suppress all wire and electronic surveillance evidence (filed December 2, 2014). Defendant's motion to suppress is denied.

BACKGROUND

According to the Government, in the spring of 2012, a law enforcement task force began investigating a conspiracy to distribute methamphetamine and collect "tax" money from drug dealers that operated with associates both inside and outside state and local detention and prison custodial facilities. As a result of the investigation, approximately 70 individuals have been charged. During the investigation, a number of wiretap orders were applied for and issued by judges in this and other United States District Courts.

Defendant now seeks to suppress evidence of telephone conversations

12

11

13

14 15

16

23

27

28

between himself and others discussing the smuggling of drugs into Donovan State Prison and collecting "taxes" for the sale and distribution of those drugs inside the prison. According to the Indictment, Defendant was an inmate in a California state prison. According to the motion, the fifth, sixth, seventh, eighth, and ninth wiretaps purport to have intercepted Defendant's communications. All nine wiretap orders in this district were issued by United States District Judges Hon. Irma E. Gonzalez and Thomas J. Whelan. Defendant does not identify a particular interception for which he seeks suppression. Defendant asserts that each wiretap order was based on a Title III wiretap application lacking the required showing of necessity. The Government does not contest Defendant's standing to challenge the admissibility of wiretap evidence.

THE FOURTH AMENDMENT DOES NOT PROTECT CELLULAR TELEPHONE COMMUNICATIONS BY A PRISONER I.

Defendant does not argue a Fourth Amendment right to suppression of his telephone conversations. Nevertheless, it is important to note that in most cases the Fourth Amendment protects the rights of the people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Its protection extends to telephone conversations and requires the government to obtain a warrant before electronically eavesdropping.

However, the protection applies only if a person has a reasonable expectation of privacy in not having his words or conversation overheard. See Katz v. United States, 389 U.S. 347 (1967). No court has ruled that a prison inmate has a reasonable expectation of privacy for communications he makes by cellular telephone. Defendant cites no case. Indeed, the United States Supreme Court decided that the Fourth Amendment proscription against unreasonable searches does not apply to a person within the walls of the prison cell. See Hudson v. Palmer, 468 U.S. 517, 525-26 (1984) ("[W]e hold that society is not prepared to recognize as legitimate any subjective expectation of privacy that a prisoner might

have in his prison cell and that, accordingly, the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell. The recognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions.").

Under *Palmer*, Defendant has no Fourth Amendment right to privacy while incarcerated upon which to base a motion to suppress evidence.

II. A COMMUNICATION THROUGH USE OF A CONTRABAND CELL PHONE BY A PRISONER IS NOT COVERED BY 18 U.S.C. § 2518 ("TITLE III")

Defendant argues that the wiretap application supporting each wiretap order, which led to the interception of his cellular telephone communications, did not satisfy Title III. See Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. ("The Wiretap Act" or "Title III"). As a general matter, Title III prohibits electronic surveillance by the federal government except under defined circumstances. The Act also provides for suppression of evidence in three instances enumerated in 18 U.S.C. § 2518(10)(a). Defendant implicitly relies on that section to suppress.

Whether Title III applies to cellular telephone communications by or between prison inmates is a question of first impression. Title III was enacted in 1968, before the invention of the cellular telephone. It was enacted to protect the Fourth Amendment right to privacy for a telephone conversations (as recognized in *Katz v. United States*, 389 U.S. 347 (1967)). *See Gelbard v. United States*, 408 U.S. 41, 47 (1972) (legislative history is clear that Congress was concerned about "safeguard[ing] the privacy of innocent persons."); *see also United States v. Forrester*, 616 F.3d 929, 945 (9th Cir. 2010) ("Supreme Court has routinely acknowledged that § 2518 . . . was enacted specifically to meet the constitutional requirements for electronic surveillance enunciated by the Supreme Court in *Berger*

[v. New York] and Katz v. United States."). While there have been more recent amendments, Title III still does not specifically mention cellular telephones.

The Ninth Circuit has acknowledged that a conventional wiretap order may apply to a cellular telephone in ordinary circumstances, and that a "roving wiretap" order is not required for a cell phone even though a cell phone has no fixed location. See United States v. Oliva, 705 F.3d 390, 400-01 & n.4 (9th Cir. 2012) ("As noted earlier, under Title III, the district court may authorize a standard intercept of communications over a land line or cellular telephone only if the government's application includes 'a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted.' § 2518(1)(b)(ii)."); see also United States v. Goodwin, 141 F.3d 394, 403 (2nd Cir. 1997) (assuming that Title III applies to cellular telephones and deciding that for a cellular telephone, the Government did not need to obtain a "roving wiretap."). But no court has addressed the applicability of Title III to a cellular telephone being used by a prisoner.

And no court has considered the impact of Congressional action in 2010 defining a mobile phone to be contraband for federal prisoners. *See* Cell Phone Contraband Act of 2010, P. L. 111-225 [S 1749], August 10, 2010 (amending 18 U.S.C. § 1791); *see also* Statement by Senator Feinstein, 155 Cong. Rec. S10112-01, 2009 WL 3171677 ("This bill would close this loophole by defining cell phones as contraband material under Federal law. As a result, any person smuggling or in possession of a cell phone could potentially serve up to a year in prison. A cell phone should never be in the hands of a prisoner. The presence of these cell phones poses a grave safety concern for staff, inmates, and the public. We know that inmates use these phones to conduct criminal business outside of prison walls, including directing gang hits, controlling drug trafficking operations and even conducting credit card fraud.").

Since the 2010 amendment to 18 U.S.C. § 1791, it has been unlawful for a

prisoner in a federal prison to possess or use a cell phone. See § 1791(d)(1)(F) defining a prohibited object as "a phone or other device used by a user of commercial mobile service. . . . "A Westlaw search found only two unpublished cases involving violations of the Cell Phone Contraband Act. See United States v. Drakes, __Fed. App'x. __, 2014 WL 6676994 (11th Cir. Nov. 26, 2014) (reviewing sentence of former federal prison guard convicted of smuggling seven cell phones into prison for resale to inmates.); United States v. Gadsden, Case No 09-305, slip op., 2012 WL 4973412 (W.D. Pa. Oct. 17, 2012) (pretrial order denying severance of counts with one count alleging possession of a prohibited object (a cellular telephone) in violation of § 1791(b)(4)). Neither case considered whether the Wiretap Act applied to conversations by inmates using contraband cellular telephones.

This Court finds that Congress created an implicit exception to the requirements of Title III. Title III does not apply to the interception by law enforcement officers of a telephone communication from a prisoner using a contraband cellular telephone. *Cf. Mitchum v. Foster*, 407 U.S. 225, 235 (1972) (describing numerous implied exceptions to the anti-injunction statute (28 U.S.C. § 2283)); *Feres v. United States*, 340 U.S. 135 (1950) (finding an implied exception to the Federal Tort Claims Act for injuries to servicemen where the injuries are incident to service); *McMellon v. United States*, 387 F.3d 329, 349 (4th Cir. 2004) (holding recent Suits in Admiralty Act (46 U.S.C. App. §§741-52) must be read to include an implied discretionary function exception to its waiver of sovereign immunity, as in the older Federal Tort Claims Act).

Passage of the Cell Phone Contraband Act makes clear that Congress considered it dangerous for an inmate to possess a cellular telephone. The potential for criminality is large. In this case, the allegations of the indictment (if true) aptly illustrate some of the dangers: orchestrating assaults on other inmates, planning contraband drug sales within the prison, ordering the transfer of drug proceeds in

outside accounts, surveillance of other inmates, carrying out a criminal conspiracy, and doing all of the above while avoiding detection by prison guards. And the use of smuggled cellular telephones by prison inmates has become a large national problem.

In federal institutions and prison camps, GAO reports that the number of cell phones confiscated by the Federal Bureau of Prisons (BOP) grew from 1,774 in 2008 to 3,684 in 2010. While not all states track or report data on the use of contraband wireless devices, the data that has been reported demonstrates significant growth. For example, California correctional officers seized approximately 261 cell phones in 2006; by 2011, correctional officers discovered more than 15,000 contraband wireless devices. Further, a test of an interdiction technology in two California State prisons detected more than 25,000 unauthorized communication attempts over an 11 day period in 2011. A similar interdiction system permanently installed in a Mississippi correctional facility reportedly blocked 325,000 communications attempts in the first month of operation, and as of February 2012, had blocked more than 2 million communications attempts.

Promoting Technological Solutions to Combat Contraband Wireless Device Use in Corr. Facilities, F.C.C. Notice of Proposed Rulemaking, 28 F.C.C. Rcd. 6603, 6607 2013 WL 1855953 *3 (2013); see also E. Fitzgerald, CELL "BLOCK" SILENCE: WHY CONTRABAND CELLULAR TELEPHONE USE IN PRISONS WARRANTS FEDERAL LEGISLATION TO ALLOW JAMMING TECHNOLOGY, 2010 Wis. L. Rev. 1269, 1276-77 (citations omitted).

22 Fitzgerald v

Cell phone smuggling is difficult to prevent because the devices are brought into correctional facilities in a myriad of ways. Inmates coordinate smuggling efforts with corrupt correctional facility workers, visiting family members, or fellow gang members. Smugglers often throw handsets over facility walls or conceal them in packages sent to the prisons. One facility in Texas reported finding seventy-five cell phones hidden in an air compressor. Smugglers opened the metal tank, hid the phones and chargers with some narcotics, and then welded the tank shut. Officials found the phones when drug-sniffing dogs detected the narcotics. The San Francisco Chronicle reported that "more than half the phones in prisons come from staff at the facilities - including guards, cooks, [and] health care workers." Correctional facility staff is familiar with the facilities in which they work, and, in some cases, undergo less

It would be an ironic interpretation of the law to find that a prison inmate,

who by virtue of his initial crime and conviction, when he is placed in a cellblock

where he has no Fourth Amendment rights, and when he commits a further crime by

obtaining and using a contraband cellular telephone, acquires a statutory right under

telephone communications, he enjoys a statutory right to suppression under Title III.

contraband cellular phone to communicate with others about a criminal conspiracy,

and he enjoys protection from those communications being recorded and admitted

against him in court, unless a valid wiretap order was in place.² This cannot be

Title III to be free from law enforcement eavesdropping, unless a Title III wiretap

order is first obtained. Yet, this is the implicit argument. Defendant argues that,

even if he does not hold a constitutional right to privacy for his contraband

His implicit argument maintains that he has a statutory right to illicitly use a

It must be the case that Congress intended to except from the purview of Title III's law enforcement restrictions, the interception of contraband cellular telephone communications from or to an inmate within a jail or prison. Therefore, because

17

18

19

20

21

22

23

24

25

26

12

13

14

15

16

what Congress intended.

stringent security requirements than visitors. In 2009, 300 California correctional employees were disciplined for suspected cell phone smuggling. 150 more have been disciplined in 2010. One California correctional officer told officials that he made more than \$100,000 in one year by smuggling cell phones. Since 2007, 230 Texas correctional facility employees have been disciplined for "cell phone-related infractions." Family members are also often culprits. Richard Tabler's mother and sister allegedly assisted him in procuring the cellular phone he used to call Senator Whitmire. They were later indicted on charges of assisting an inmate to obtain a contraband cell phone. The cost to procure a cell phone on the black market varies widely depending on prison location and an inmate's level of security, but is within reach for criminals continuing to engage in profitable criminal enterprises. On the high end, Texas death row inmate Tabler paid \$2100 for his contraband cell phone. California officials note that contraband cell phones can be purchased for between \$100 and \$400 each. Family or gang members often cover the initial financial outlay and subscription rates.

²⁷ 28

²It makes no difference that Defendant was an inmate in a California state or local facility, rather than a federal prison, because California law also treats possession and use of a cellular phone by an inmate as a misdemeanor crime. *See* Cal. Penal Code §§ 4575 & 4576.

Title III implicitly excepts law enforcement officers from the need to obtain a wiretap order before intercepting or recording an inmate's contraband cell phone communications, Defendant's motion to suppress such recordings under Title III is denied.

III. ALTERNATIVELY, THE DECISION OF THE DISTRICT JUDGE ISSUING A WIRETAP ORDER IS ENTITLED TO DEFERENCE FROM ANOTHER DISTRICT JUDGE CONSIDERING A MOTION TO SUPPRESS

When a United States District Judge reviews a Title III wiretap application and concludes that law enforcement has made a proper case and issues a wiretap order, that decision is accorded a measure of deference by the court of appeals. *United States v. Rivera*, 527 F.3d 891, 904 (9th Cir. 2008) ("[W]e may not reverse simply because we might have decided not to grant the wiretap. We review the issuing court's decision to grant the wiretap for an abuse of discretion."); *United States v. Lynch*, 437 F.3d 902, 912 (9th Cir. 2006) (en banc) ("[T]he conclusion that the wiretap was necessary in each situation is reviewed for abuse of discretion."); *United States v. Canales Gomez*, 358 F.3d 1221, 1225 (9th Cir. 2004) ("The issuing judge's decision that the wiretap was necessary is reviewed under an abuse of discretion standard."). The correct standard of review for a district court to use when judging a motion to suppress, however, has not been identified by the parties and the Ninth Circuit has not directly addressed the question.

Some district courts have implicitly reviewed wiretap orders *de novo*. Other district courts have applied an abuse of discretion standard. *See United States v. Yim*, No. CR11-131-MJP, 2012 WL 395791 *5 (W.D. Wash. Feb 7, 2012) (citations omitted) ("Defendants argue that the Court should apply a de novo review to the showing of necessity. Defendants cite no case that stands for that proposition, but urge the Court to do so because this is the first time the allegations as to necessity are subjected to an adversarial challenge. The Court is not persuaded by this

argument, given the fact this Court sits in the same position as the Ninth Circuit 1 when reviewing an affidavit's showing of necessity. Both before this Court and the 2 Ninth Circuit, the warrant has issued, the arrests have been made, and the 3 adversarial process commenced. Prior to that, it is up to the reviewing judge to use her discretion to gauge whether the affidavit sustains a showing of necessity and that determination is entitled to deference under an abuse of discretion standard. The Court thus applies the abuse of discretion standard in analyzing the issue of 7 necessity."); United States v. Velarde-Ozuna, No. CR10-754-TUC-CKJ, 2011 8 WL5007918 *2 (D. Ariz. Oct. 20, 2011) ("An appellate court reviews an 'issuing judge's decision that the wiretaps were necessary for an abuse of discretion.' A 10 district court evaluating a wiretap authorization in order to resolve a suppression 11 motion applies the same standard of review."); United States v. Ai Le, 255 F. Supp. 12 2d 1132, 1134 (E.D. Cal. 2003) (citations omitted) ("[A] court reviewing a wiretap 13 authorization must use an abuse of discretion standard."). These decisions are 14 better reasoned and persuasive. Consequently, this Court will not suppress wiretap 15 evidence simply because it might have adjudged the wiretap application differently 16 than did an issuing judge. The decision to issue a wiretap order will be accorded a 17 measure of deference. Only if there is a clear and convincing case made that the 18 wiretap order was the result of the issuing judge's abuse of discretion, will this 19 Court grant a motion to suppress. 20 21

Defendant makes no argument that the judge who issued the wiretap order in this case in any way abused her discretion. She had the lengthy wiretap application and the application arguably supported the order. She could arguably find probable cause to believe a crime was being committed. She could arguably find that other investigative tools had been tried and a wiretap was necessary to extirpate the criminal conspiracy. She could arguably find that the wiretap request was sufficiently confined. In short, Defendant has identified no reason, and this Court finds there is no reason, to conclude that the issuing judge's decision is not entitled

22

23

24

25

26

27

28

to deference. Defendant's argument now, that the wiretap order should not have 1 2 3

been issued because the application was deficient, without much more, is foreclosed. Therefore, the motion to suppress is denied.

4

5

ALTERNATIVELY, THE GOVERNMENT MADE A SUFFICIENT SHOWING OF NECESSITY IN THE WIRETAP APPLICATION IV.

6

7

8

9

10

11

Assuming for the sake of argument, that Defendant, using a contraband cell phone while incarcerated, has a constitutional or statutory right to suppress evidence gained in violation of Title III, and assuming for the sake of argument that no deference is to be given the decision of the wiretap-issuing district judge, Defendant has still failed to carry his burden of proving a wiretap order was defective.

The Wiretap Act provides three grounds upon which evidence derived from a

12 13

14

unlawfully intercepted." See 18 U.S.C. 2518(10)(a)(i). Second, it may be proven that, "the order or authorization or approval under which it was intercepted is

wiretap may be suppressed. First, it may be proven that, "the communication was

15 16

insufficient on its face." See 18 U.S.C. 2518(10)(a)(ii). Third, it may be proven

17

that, "the interception was not made in conformity with the order of authorization or

18 19 approval." See 18 U.S.C. 2518(10)(a)(iii). Defendant has not specified the basis upon which he seeks suppression.

20

When a court is reviewing "necessity," the Ninth Circuit has adopted a "common sense approach to evaluate the reasonableness of the government's good

22

21

faith efforts to use traditional investigative tactics or its decision to forego such

23

tactics based on the unlikelihood of their success or the probable risk of danger involved with their use." United States v. Garcia-Villalba, 585 F.3d 1223, 1228

24 25

(9th Cir. 2009) (citations and internal quotations omitted). When investigating a

26

criminal conspiracy, the government is given "more leeway in its investigative methods.." Id. at 1230. "Like the Hydra of Greek Mythology . . . the conspiracy

27

28

may survive the destruction of its parts unless the conspiracy is completely

destroyed." *Id.* (quoting *United States v. McGuire*, 307 F.3d 1192, 1197-98 (9th Cir. 2002). This is because, the Ninth Circuit has observed, "it is one of the first duties of every government to extirpate gangs of thieves." *Id.*

A. Omissions in the Affidavit

g

Defendant argues that the agent's affidavit supporting the application for a wiretap "does not detail each and every fact learned during the course of the investigation." He suggests that the agent may have left out facts, but does not identify any specific omitted facts. A Defendant seeking suppression on the basis of a misstatement or omission must satisfy several requirements, including a detailed offer of proof and an affidavit, before going forward under *Franks v. Delaware*, 43 U.S. 154, 155-56 (1978). *United States v. Perdomo*, 800 F.2d 916, 920 (9th Cir. 1986) (listing five requirements for a *Franks* hearing); *United States v. Gutierrez*, No. 12CR236-IEG, 2012 WL 6624769*1-4 (S.D. Cal. Dec. 19, 2012) (describing requirements for *Franks* hearing for wiretaps). Defendant has not satisfied these requirements.

B. Broad Goals of the Investigation

Defendant argues that the government's stated goal of the investigation was overly broad to the point of being flawed. However, the Ninth Circuit has approved in other cases similarly broad investigative goals in drug smuggling conspiracies. *See Canales Gomez*, 358 F.3d at 1224; *United States v. Shryock*, 342 F.3d 948, 975-76 (9th Cir. 2003); *see also United States v. Chan*, No. C 05-375 SI, 2006 WL 1581946*6 (N.D. Cal. June 6, 2006) (denying motion to suppress wiretap evidence where investigatory goals of identifying conspirators and methods were very broad.). He notes that the Government may not adopt investigatory goals "so far and so wide" that the goals can be seen as "manufactur[ing] necessity in all circumstances." *United States v. Blackmon*, 273 F.3d 1204, 1211 (9th Cir. 2000). In *Blackmon*, the principal problem was that the Title III application contained material omissions and misstatements. When "purged of these misstatements...

the remainder of the application, which contain[ed] generalized statements that
would be true of any narcotics investigation, fail[ed] to contain sufficiently specific
facts to satisfy the requirements of § 2518(1)(c)." *Id.* In this case, the Government
did not cast its net so far and so wide as to have manufactured necessity in every
circumstance. Instead, it adopted an investigatory goal that was limited to a
narcotics distribution and taxation conspiracy operated in California Prisons and
jails. The applications in this case do not have the same flaws as the *Blackmon*application.

C. Alternative and Less Intrusive Techniques

Defendant's main thrust is that there were less intrusive investigative techniques that could have been tried as an alternative to wiretaps. For example, Defendant discusses recorded jail calls, confidential informants, surveillance, tracking devices, grand jury subpoenas, searches, mail covers, undercover agents, and pen registers.

But the Government need not exhaust every possible means of investigation before seeking a wiretap authorization. The Ninth Circuit has said that a wiretap should not ordinarily be the first step in an investigation, "but that law enforcement officials need not exhaust every conceivable alternative before obtaining a wiretap." *United States v. McGuire*, 307 F.3d 1192, 1196-97 (9th Cir. 2002). Here, the Government used a variety of traditional investigatory techniques before seeking wiretaps. It was not obligated to use that which Defendant, now, suggests would have been effective. This argument is not enough.

D. Confidential Informants

Defendant argues that the investigators had used confidential informants successfully. He criticizes the government for not waiting for new informants to appear and suggests that the government should have tried inserting a undercover agent before resorting to a wiretap.

The Ninth Circuit has explained that "the use of informants to investigate and

prosecute persons engaged in clandestine criminal activity is fraught with peril." Canales Gomez, 358 F.3d at 1226 (quoting United States v. Bernal-Obeso, 989 F.2d 2 331, 333 (9th Cir. 1993)). Informants are often untrustworthy and unattractive to a 3 jury. "There is not a trial lawyer alive who does not understand that juries are wary of any witness receiving a benefit for testifying." Id. at 1227. In this case, the 5 confidential informant committed another serious crime during the time when the 6 government was investigating its case against this defendant. The informant's unrestrained and unsanctioned criminal activity gave the investigators good reason 8 to discontinue the employment of the informant. "The truth-seeking function of our courts is greatly enhanced when the evidence used is not tainted by its immediate 10 informant source and has been cleansed of the baggage that always comes with 11 them." Id. In contrast to the testimony of informants, "wiretap evidence out of the 12 mouths of defendants is valuable corroboration of informant testimony [and] 13 serves to ensure that what investigators are being told by informants is accurate, a 14 very valuable function that guards the indictment of the innocent." Id. In light of 15 these investigatory concerns, the Ninth Circuit has said, "a reasoned review of a 16 wiretap request must take into account the added difficulty, expense, and danger of 17

18

19

20

21

22

23

24

25

26

27

28

E. Pre-Wiretap Investigation Success

Defendant argues that investigators had achieved every reasonable goal of their investigation prior to seeking the wiretaps, and that therefore, the wiretaps were not necessary. A similar argument was dismissed by the Ninth Circuit. Even if an investigation has been successful enough to gain an indictment against one conspirator, "it is plain beyond doubt that the existence of an indictment does not make wiretapping unnecessary." *Id.* at 1198. A wiretap may be necessary so that the Government may develop "evidence of guilt beyond a reasonable doubt, not merely evidence sufficient to secure an indictment." *Id.* Finally, possession of

using informants, especially those concurrently charged with other crimes." Id.

The government, in this case, has made a sufficient showing of necessity.

Case 3:13-cr-04514-JO

Document 216

Filed 02/03/15

PageID.1523

Page 14 of